CYCLOTOMY AND PERMUTATION POLYNOMIALS OF LARGE INDICES

QIANG WANG

Abstract. We use cyclotomy to design new classes of permutation polynomials over finite fields. This allows us to generate many classes of permutation polynomials in an algorithmic way. Many of them are permutation polynomials of large indices.

1. Introduction

Let p be prime and $q = p^m$. Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. A polynomial is a permutation polynomial (PP) of a finite field $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ to itself. The study of permutation polynomials of a finite field goes back to 19-th century when Hermite and later Dickson pioneered this area of research. In recent years, interests in permutation polynomials have significantly increased because of their applications in coding theory and cryptography such as S-boxes. In some of these applications, the study of permutation polynomials over finite fields has also been extended to the study of permutation polynomials over finite rings and other algebraic structures. For more background material on permutation polynomials we refer to Chap. 7 of [11]. For a detailed survey of open questions and recent results see [9], [10], [12], and [13].

In [3], the authors provide a general theory which, in essence, reduces a problem of determining whether a given polynomial over a finite field $\mathbb{F}_q$ is a permutation polynomial to a problem of determining whether another polynomial permutes a smaller set. One of very useful smaller sets is the set of cyclotomic cosets. Earlier, Niederreiter and Winterhof [15] and Wang[17] have studied so-called cyclotomic permutations. Namely, let C_0 be a subgroup of $\mathbb{F}_q^*$ with index $\ell \mid q-1$ and the factor group $\mathbb{F}_q^*/C_0$ consists of the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i = 0, 1, \cdots, \ell - 1,$$

where γ is a fixed primitive element of $\mathbb{F}_q$. For any $A_0, A_1, \cdots, A_{\ell-1} \in \mathbb{F}_q$ and positive integer r, the so-called *r-th order cyclotomic mapping $f^r_{A_0,A_1,\cdots,A_{\ell-1}}$ of index ℓ* from $\mathbb{F}_q$

2000 *Mathematics Subject Classification.* 11T06.

Key words and phrases. polynomials, permutation polynomials, cyclotomic mappings, finite fields.

Research of the authors was partially supported by NSERC of Canada.

to itself is defined by

$$f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases}0, & if\ x=0;\\ A_0x^r, & if\ x\in C_0;\\ \vdots & \vdots\\ A_ix^r, & if\ x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}x^r, & if\ x\in C_{\ell-1}.\end{cases}$$

It is shown that r-th order cyclotomic mappings produce the polynomials of the form $x^rf(x^s)$ where $s=\frac{q-1}{\ell}$. Furthermore, PPs of the form $x^rf(x^s)$ have been intensively studied in [1, 2, 4, 5, 6, 7, 16, 17, 21, 22, 23].

It is also well known that every polynomial $P(x)$ over $\mathbb{F}_q$ such that $P(0)=b$ has the form $ax^rf(x^s)+b$ with some positive integers r,s such that $s\mid q-1$. Let $q-1=\ell s$. More precisely, we observe that any polynomial $P(x)\in\mathbb{F}_q[x]$ can be written as $a(x^rf(x^{(q-1)/\ell}))+b$, for some $r\geq 1$ and $\ell\mid(q-1)$. To see this, without loss of generality, we can write

$$P(x)=a(x^n+a_{n-i_1}x^{n-i_1}+\cdots+a_{n-i_k}x^{n-i_k})+b,$$

where $a,\ a_{n-i_j}\neq 0,\ j=1,\cdots,k$. Here we suppose that $j\geq 1$ and $n-i_k=r$. Then $P(x)=a\left(x^rf(x^{(q-1)/\ell})\right)+b$, where $f(x)=x^{e_0}+a_{n-i_1}x^{e_1}+\cdots+a_{n-i_{k-1}}x^{e_{k-1}}+a_r$,

$$\ell=\frac{q-1}{\gcd(n-r,n-r-i_1,\cdots,n-r-i_{k-1},q-1)},$$

and $\gcd(e_0,e_1,\cdots,e_{k-1},\ell)=1$. The constant ℓ is called the *index* of polynomial $P(x)$ (see [2]). The index of a polynomials is closely related to the concept of the least index of cyclotomic permutations. Many classes of PPs that are constructed recently have small indices ℓ, see for example, [1, 4, 5, 6, 7, 21, 22].

In this paper, we extend the definition of cyclotomic mappings and study the permutation polynomials corresponding to these cyclotomic mappings. These polynomials have either the presentation given in terms of cyclotomic mappings of index ℓ,

$$f^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases}0, & if\ x=0;\\ A_0r_0(x), & if\ x\in C_0;\\ \vdots & \vdots\\ A_ir_i(x), & if\ x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}r_{\ell-1}(x), & if\ x\in C_{\ell-1},\end{cases}$$

or the polynomial presentation

$$P(x)=\sum_{i=0}^{\ell-1}\frac{A_i}{\ell\zeta^{i(\ell-1)}}r_i(x)\left(x^{(\ell-1)s}+\zeta^ix^{(\ell-2)s}+\cdots+\zeta^{i(\ell-2)}x^s+\zeta^{i(\ell-1)}\right),$$

where $r_0(x),r_1(x),\ldots,r_{\ell-1}(x)\in\mathbb{F}_q[x]$ and $\zeta=\gamma^s$ be a fixed primitive ℓ-th root of unity throughout this paper. Essentially, these polynomials are of the form $\sum_{i=0}^n x^{r_i}f_i(x^s)$.

And indices of polynomials of this form are normally large, which are different from ℓ in general. After we study several cases when $r_i(x)$'s are general and ℓ is small, we study in detail the situation when $r_i(x)$'s are monomials x^{r_i} for some positive integers r_i's. We give some general criteria of determining these polynomials are permutation polynomials of finite fields (Theorems 2.18, 2.19, 3.1, 3.2). One of them can be written as follows:

Theorem 1.1. *Let $q-1=\ell s$ and $A_0,\ldots,A_{\ell-1}\in\mathbb{F}_q$. Then*

$$P(x)=\begin{cases}0, & if\ x=0;\\ A_0x^{r_0}, & if\ x\in C_0;\\ A_1x^{r_1}, & if\ x\in C_1;\\ \vdots & \vdots\\ A_{\ell-1}x^{r_{\ell-1}}, & if\ x\in C_\ell,\end{cases}$$

is a PP of $\mathbb{F}_q$ if and only if $(r_i,s)=1$ for any $i=0,1,\ldots,\ell-1$ and $\mu_\ell=\{A_i^s\zeta^{r_ii}\mid i=0,\ldots,\ell-1\}$, where μ_ℓ is the set of all ℓ-th roots of unity.

We note that each $A_i^s\zeta^{r_ii}$ is an ℓ-th root of unity as long as A_i is not zero. Hence what we really need is to check all $A_i^s\zeta^{r_ii}$ $(0\le i\le\ell-1)$ are distinct in the above theorem. Using these criteria in different forms, we demonstrate our method by constructing many new classes of PPs (Theorems 2.4, 2.6, 2.13, 2.14, 2.17, 3.4, 3.6, 3.8, Corollaries 3.3, 3.5, 3.7). Here we only list very few particular examples of these results over fields with small characteristic.

Theorem 1.2. *The polynomial $P(x)=x^{\frac{2(2^n-1)}{3}+2^i}+x^{\frac{2(2^n-1)}{3}+2^j}+x^{\frac{2^n-1}{3}+2^i}+x^{\frac{2^n-1}{3}+2^j}+x^{2^i}$ is a PP of $\mathbb{F}_{2^n}$ for any even positive integer n and non-negative integers i,j.*

Theorem 1.3. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+3^i}+2x^{\frac{3^n-1}{2}+3}+2x^{\frac{3^n-1}{2}+2}+2x^{\frac{3^n-1}{2}+1}+x^{3^i}+x^3+x^2+x$ is a PP of $\mathbb{F}_{3^n}$ for any positive integer n and non-negative integer i.*

Theorem 1.4. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+2^i}+2x^{\frac{3^n-1}{2}+3}+2x^{\frac{3^n-1}{2}+2}+2x^{\frac{3^n-1}{2}+1}+x^{2^i}+x^3+x^2+x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

Theorem 1.5. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+3^i}+2x^{\frac{3^n-1}{2}+3}+x^{\frac{3^n-1}{2}+2}+2x^{\frac{3^n-1}{2}+1}+2x^{2^i}+2x^3+x^2+2x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

Theorem 1.6. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+2^i}+x^{\frac{3^n-1}{2}+3}+2x^{\frac{3^n-1}{2}+2}+x^{\frac{3^n-1}{2}+1}+2x^{2^i}+x^3+2x^2+x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

Theorem 1.7. *Let $q=3^n$ and $\alpha,\beta,\gamma,\theta\in\mathbb{F}_{3^n}$. Let $f(x)=(\beta-\alpha)x^{(q-1)/2+3}+(\beta\theta-\alpha\gamma)x^{(q-1)/2+2}+(\beta\theta^2-\alpha\gamma^2)x^{(q-1)/2+1}-(\beta+\alpha)x^3-(\beta\theta+\alpha\gamma)x^2-(\beta\theta^2+\alpha\gamma^2)x$. Then f is a PP of $\mathbb{F}_{3^n}$ if and only if $\eta(\alpha)=\eta(\beta)$, $\eta(\gamma)=-1$, and $\eta(\theta)=1$.*

One can easily see from the definition that these classes of PPs have indeed large indices because they contain terms with consecutive exponents. We also remark that our results not only generalize many previous results in [1, 5, 6, 21], but also generalize several more recent results including a class of PPs constructed by Hou in the study of reversed Dickson polynomials (Theorem 1.1 in [8]) and several classes of PPs studied by Zha and Hu thereafter (Theorems 7-11 in [20]); see Theorems 2.6, 2.21, 2.22, 2.27. Our method can also provide an algorithmic way to generate permutation polynomials over finite fields.

2. Cyclotomic mappings permutation polynomials

Let γ be a fixed primitive element of $\mathbb{F}_q$, $\ell \mid q-1$, and the set of all nonzero ℓ-th powers be $C_0 = \{\gamma^{\ell j} : j = 0, 1, \cdots, s-1\}$. Then C_0 is a subgroup of $\mathbb{F}_q^*$ of index ℓ. The elements of the factor group $\mathbb{F}_q^*/C_0$ are the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i = 0, 1, \cdots, \ell-1.$$

For any $A_0, A_1, \cdots, A_{\ell-1} \in \mathbb{F}_q$ and monic polynomials $r_0(x), \ldots, r_{\ell-1}(x) \in \mathbb{F}_q[x]$ we define a *cyclotomic mapping* $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}$ *of index* ℓ from $\mathbb{F}_q$ to itself by

$$f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}(x) = \begin{cases} 0, & if\ x = 0; \\ A_0 r_0(x), & if\ x \in C_0; \\ \vdots & \vdots \\ A_i r_i(x), & if\ x \in C_i; \\ \vdots & \vdots \\ A_{\ell-1} r_{\ell-1}(x), & if\ x \in C_{\ell-1}. \end{cases}$$

Moreover, $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}$ is called an *cyclotomic mapping of the least index* ℓ if the mapping can not be written as a cyclotomic mapping of any smaller index. The polynomial of degree at most $q-1$ representing the cyclotomic mapping $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}(x)$ is called an *cyclotomic mapping polynomial*. In particular, when $r_0(x) = \cdots = r_{\ell-1}(x) = x^r$ for a positive integer r, it is known as a *r-th order cyclotomic mapping polynomial*, denoted by $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r}(x)$ (see [15] for $r = 1$ or [17]).

Let $s = \frac{q-1}{\ell}$ and $\zeta = \gamma^s$ be a primitive ℓ-th root of unity. It is shown in [6] that polynomials of the form $x^r f(x^s)$ and the r-th order cyclotomic mapping polynomials $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r}(x)$ where $A_i = f(\zeta^i)$ for $0 \le i \le \ell-1$ are the same. More generally, for any $P(x) = \sum_{i=0}^{\ell-1} r_i(x) f_i(x^s)$ with $P(0) = 0$, we can also write $P(x)$ as a cyclotomic mapping as follows:

$$P(x)=f_{A_0,A_1,\cdots,A_{\ell-1}}^{P_0(x),P_1(x)\ldots,P_{\ell-1}(x)}(x)=\begin{cases}0, & \text{if } x=0;\\ A_0P_0(x), & \text{if } x\in C_0;\\ \vdots & \vdots\\ A_iP_i(x), & \text{if } x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}P_{\ell-1}(x), & \text{if } x\in C_{\ell-1},\end{cases}$$

where $A_jP_j(x)=\sum_{i=0}^{\ell-1}r_i(x)f_i(\zeta^j)$ and $P_j(x)$ is the monic associated polynomial. Indeed, for any $x\in C_j$, $x=\gamma^{\ell i+j}$ for some $0\le i\le s-1$ and thus $P(\gamma^{\ell i+j})=\sum_{i=0}^{\ell-1}r_i(\gamma^{\ell i+j})f_i(\zeta^j)=A_jP_j(\gamma^{\ell i+j})$.

On the other hand, for any given cyclotomic mapping of index ℓ,

$$f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}(x)=\begin{cases}0, & if\ x=0;\\ A_0r_0(x), & if\ x\in C_0;\\ \vdots & \vdots\\ A_ir_i(x), & if\ x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}r_{\ell-1}(x), & if\ x\in C_{\ell-1},\end{cases}$$

we can find a unique polynomial $P(x)$ modulo x^q-x corresponding to it. Namely,

$$P(x)=\sum_{i=0}^{\ell-1}\frac{A_i}{\ell\zeta^{i(\ell-1)}}r_j(x)\left(x^{(\ell-1)s}+\zeta^ix^{(\ell-2)s}+\cdots+\zeta^{i(\ell-2)}x^s+\zeta^{i(\ell-1)}\right). \tag{1}$$

Indeed, if each $x\in C_i$, we must have $x^s=\zeta^i$. So we have

$$\frac{A_i}{\ell\zeta^{i(\ell-1)}}r_i(x)\left(x^{(\ell-1)s}+\zeta^ix^{(\ell-2)s}+\cdots+\zeta^{i(\ell-2)}x^s+\zeta^{i(\ell-1)}\right)=A_ir_i(x),$$

and for $j\neq i$,

$$\frac{A_j}{\ell\zeta^{j(\ell-1)}}r_j(x)\left(\zeta^{i(\ell-1)}+\zeta^j\zeta^{i(\ell-2)}+\cdots+\zeta^{j(\ell-2)}\zeta^i+\zeta^{j(\ell-1)}\right)=\frac{A_j(\zeta^{i\ell}-\zeta^{j\ell})}{\ell\zeta^{j(\ell-1)}(\zeta^i-\zeta^j)}r_j(x)=0.$$

The correspondence (1) provides a way to construct permutation polynomials of finite fields. First of all, it is obvious to obtain the following result on cyclotomic mappings.

Lemma 2.1. *Let $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}(x)$ be a cyclotomic mapping of index ℓ over $\mathbb{F}_q$ given as*

$$f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}(x)=\begin{cases}0, & if\ x=0;\\ A_0r_0(x), & if\ x\in C_0;\\ \vdots & \vdots\\ A_ir_i(x), & if\ x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}r_{\ell-1}(x), & if\ x\in C_{\ell-1}.\end{cases}$$

Then $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}$ *induces a permutation of* $\mathbb{F}_q$ *if and only if* $\cup_{i=0}^{\ell-1} A_i r_i(C) = \mathbb{F}_q^*$, *where* $A_i r_i(C_i) = \{A_i r_i(x) \mid x \in C_i\}$ *for* $0 \le i \le \ell-1$. *In particular, if* $A_0, \ldots, A_{\ell-1} \neq 0$ *and each* $A_i r_i(x)$ *is a bijective map from* C_i *to another coset* C_{j_i}, *then* $f_{A_0,A_1,\cdots,A_{\ell-1}}^{r_0(x),r_1(x),\ldots,r_{\ell-1}(x)}$ *induces a permutation of* $\mathbb{F}_q$ *if and only if*

$$\{A_0 r_0(C_0), \ldots, A_{\ell-1} r_{\ell-1}(C_{\ell-1})\} = \{C_0, \ldots, C_{\ell-1}\}.$$

Lemma 2.1 and Equation (1) provide us a general scheme to construct PPs of finite fields. We can design PPs of specific type in two steps. First, we choose an $\ell \mid q-1$ and set a pattern of permutation of cyclotomic cosets. For example, we may want to have a permutation which maps C_0 to C_1, C_1 to C_2, etc. Secondly, we choose different polynomials which maps one C_i to another C_j satisfying the previous requirements and use them to form a cyclotomic mapping. In the above example, we choose ℓ polynomials $A_i r_i(x)$ which map C_0 to C_1, C_1 to C_2, etc, respectively. The polynomial determined by Equation (1) is the desired one. We note that $A_i r_i(x)$'s do not need to be PPs of $\mathbb{F}_q$, they only need to be bijective from one C_i to another C_j depending on the requirements. This gives a lot of flexibility and opens up a direction of studying polynomials that map one C_i to another C_j bijectively. In the rest of paper, we demonstrate our methodology and construct many new PPs of finite fields, many of them have large indices.

First of all, we obtain the following result for cyclotomic mappings polynomials of index 2 which follows directly from Lemma 2.1.

Theorem 2.2. *Let* $A_0, A_1 \in \mathbb{F}_q$ *and* $f_0(x), f_1(x)$ *be any two polynomials of* $\mathbb{F}_q$ *such that*

$$f(x) = f_{A_0,A_1}^{f_0(x),f_1(x)}(x) = \begin{cases} 0, & if\ x = 0; \\ A_0 f_0(x), & if\ x \in C_0; \\ A_1 f_1(x), & if\ x \in C_1. \end{cases}$$

Then f *is a PP of* $\mathbb{F}_q$ *if either one of the following holds.*

(i) $A_0 f_0(C_0) = C_0$ *and* $A_1 f_1(C_1) = C_1$; *or*

(ii) $A_0 f_0(C_0) = C_1$ *and* $A_1 f_1(C_1) = C_0$.

In particular, if we take $f_1(x), f_2(x)$ as any two polynomials of $\mathbb{F}_q$ of indices at most 2, then we have the following.

Theorem 2.3. *Let* q *be odd and let* r_0, r_1 *be positive integers and* $f_0(x), f_1(x) \in \mathbb{F}_q[x]$. *Let*

$$f(x) = \begin{cases} 0, & if\ x = 0; \\ x_0^r f_0(x^{(q-1)/2}), & if\ x \in C_0; \\ x_1^r f_1(x^{(q-1)/2}), & if\ x \in C_1. \end{cases}$$

Then f *is a PP of* $\mathbb{F}_q$ *if and only if* $(r_0, (q-1)/2) = (r_1, (q-1)/2) = 1$ *and* $\eta(f_0(1) f_1(-1)) = (-1)^{r_1+1}$, *where* η *is a quadratic character of* $\mathbb{F}_q$.

Proof. Obviously $f_0(x^{(q-1)/2}) = f_0(1)$ for $x \in C_0$ and $f_1(x^{(q-1)/2}) = f_1(-1)$ for $x \in C_1$. If f is a PP, we must have $(r_0, (q-1)/2) = (r_1, (q-1)/2) = 1$. Moreover, $f_0(1) x^{r_0}$

maps C_0 onto C_0 if $\eta(f_0(1)) = 1$, and onto C_1 if $\eta(f_0(1)) = -1$. Therefore $f_1(-1)x^{r_1}$ maps C_1 onto C_1 if $\eta(f_1(-1)) = (-1)^{r_1+1}$, and onto C_0 if $\eta(f_1(-1)) = (-1)^{r_1}$. In any case, $\eta(f_0(1)f_1(-1)) = (-1)^{r_1+1}$. The converse is obvious and we omit the proof. □

The following result generalizes Theorem 8 [20] which only gives the sufficient part.

Theorem 2.4. *Let p be an odd prime and n, t, r be any positive integers. Then $f(x) = (1-x^t)x^{\frac{p^n-1}{2}+r} - x^r - x^{t+r}$ is a PP over $\mathbb{F}_{p^n}$ if and only if $(r, p^n-1) = 1$ and $(t+r, \frac{p^n-1}{2}) = 1$.*

Proof. We rewrite $f(x) = (1-x^t)x^{\frac{p^n-1}{2}+r} - x^r - x^{t+r} = x^r(x^{\frac{p^n-1}{2}} - 1) - x^{r+t}(x^{\frac{p^n-1}{2}} + 1)$. Obviously $s = \frac{p^n-1}{2}$, $\ell = 2$, $r_0 = t+r$, $f_0(x) = -(x+1)$, $r_1 = r$ and $f_1(x) = x-1$. So we write $f(x) = f_{-2,-2}^{x^{r+t},x^r}(x)$. By the previous theorem, f is a PP if and only if $(r, (p^n-1)/2) = 1$, $(t+r, (p^n-1)/2) = 1$, and $(r, 2) = 1$. □

If $(t+r, \frac{p^n-1}{2}) = 1$ and $(t+r, p^n-1) = 2$, then we must have $p^n \equiv 3 \pmod 4$. Hence we have the following corollary.

Corollary 2.5 (Theorem 8 [20])**.** *Let p be an odd prime and n, t, r be any positive integers. Then $f(x) = (1-x^t)x^{\frac{p^n-1}{2}+r} - x^r - x^{t+r}$ is a PP over $\mathbb{F}_{p^n}$ provided*

(i) $(r, p^n-1) = 1$ and $(t+r, p^n-1) = 1$; or

(ii) $(r, p^n-1) = 1$, $(t+r, p^n-1) = 2$ and $p^n \equiv 3 \pmod 4$.

Next we obtain the following new classes of PPs over finite fields of characteristic 3.

Theorem 2.6. *Let $q = 3^n$ and t be any positive integer. Let $\alpha, \beta, \theta \in \mathbb{F}_q^*$ and*

$$f(x) = \begin{cases} 0, & if\ x = 0; \\ \alpha x^t, & if\ x \in C_0; \\ \beta(x^3 + \theta x^2 + \theta^2 x), & if\ x \in C_1. \end{cases}$$

Then f is a PP of $\mathbb{F}_q$ if and only if $(t, \frac{q-1}{2}) = 1$, $\eta(\theta) = 1$, and $\eta(\alpha) = \eta(\beta)$, where η is the quadratic character of $\mathbb{F}_q$. In this case, $f(x) = (\beta x^3 + \beta\theta x^2 + \beta\theta^2 x - \alpha x^t)x^{\frac{3^n-1}{2}} - (\beta x^3 + \beta\theta x^2 + \beta\theta^2 x + \alpha x^t)$.

Proof. Assume f is a PP. Because x^t always map C_0 into C_0 and $\beta(x^3 + \theta x^2 + \theta^2 x) = \beta x(x-\theta)^2$, we must have $\eta(\alpha) = \eta(\beta)$. Indeed, we must have either $\eta(\alpha) = \eta(\beta) = 1$ so that f maps C_0 into C_0 and maps C_1 into C_1, or $\eta(\alpha) = \eta(\beta) = -1$ so that f maps C_0 into C_1 and maps C_1 into C_0. In either case, $(t, \frac{q-1}{2}) = 1$ because x^t permutes C_0. On the other hand, let $\beta(x^3+\theta x^2+\theta^2 x) = \beta(y^3+\theta y^2+\theta^2 y)$ for $x, y \in C_1$. Then we obtain $(x-y)(x^2+(y-2\theta)x+(y-\theta)^2) = 0$. It is obvious that $(x^2+(y-2\theta)x+(y-\theta)^2) = 0$ if and only if $\eta((y-2\theta)^2 - 4(y-\theta)^2) = \eta(\theta y) = 1$. Hence $\beta(x^3+\theta x^2+\theta^2 x)$ is one-to-one over C_1 if and only if $(x^2 + (y-2\theta)x + (y-\theta)^2) \neq 0$ over C_1. The latter is equivalent to $\eta(\theta y) \neq 1$ and thus $\eta(\theta) = 1$. The converse is similar and we omit the proof. □

We note that in the case that $\theta = 0$, f is a PP of $\mathbb{F}_q$ if and only if $(t, \frac{q-1}{2}) = 1$ and $\eta(\alpha) = \eta(\beta)$.

In the study of permutation behaviour of the reversed Dickson polynomial, Hou [8] proved that $D_{3^e+5}(1,x)$ is a PP over $\mathbb{F}_{3^e}$ when e is positive even integer. Equivalently, Hou proved the following result which can also be put into the context of cyclotomic mappings. We observe that Hou's result follows from Theorem 2.6 for $t=3$, $\alpha=\theta=2$ and $\beta=1$ (with a linear shift by -1). We note that $\eta(2)=\eta(1)=1$ in $\mathbb{F}_{3^e}$ for any even positive e.

Corollary 2.7 (Theorem 1.1, [8])**.** *Let e be a positive even integer. Then $f(x)=(1-x-x^2)x^{\frac{3^e+1}{2}}-1-x+x^2$ is a PP over $\mathbb{F}_{3^e}$.*

Similarly, let $t=3^i$, $\alpha=\beta=2$ and $\theta=1$, we have the following result.

Theorem 2.8. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+3^i}+2x^{\frac{3^n-1}{2}+3}+2x^{\frac{3^n-1}{2}+2}+2x^{\frac{3^n-1}{2}+1}+x^{3^i}+x^3+x^2+x$ is a PP of $\mathbb{F}_{3^n}$ for any positive integer n and non-negative integer i.*

In particular, when $i=1$, we have

Corollary 2.9. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+2}+x^{\frac{3^n-1}{2}+1}+x^3+2x^2+2x$ is a PP over $\mathbb{F}_{3^n}$ for any positive integer n.*

The following result (Proposition 1 in [20]) follows also from Theorem 2.6 for $\alpha=1$. We note $(t,3^n-1)=1$ implies that t is odd and thus $(t,(3^n-1)/2)=1$.

Corollary 2.10. *Let t be a positive integer with $(t,3^n-1)=1$. Assume $\theta,\beta\in\mathbb{F}_{3^n}^*$ with $\eta(\theta)=\eta(\beta)=1$. Then $f(x)=(\beta x^3+\beta\theta x^2+\beta\theta^2x-x^t)x^{\frac{3^n-1}{2}}-(\beta x^3+\beta\theta x^2+\beta\theta^2x+x^t)$ is a PP over $\mathbb{F}_{3^n}$.*

Theorem 2.6 generalizes Proposition 1 in [20] in a few different ways. First, it gives a necessary and sufficient description. Secondly, a constant α could be interpreted as $f_i(x^{(q-1)/2})$ for any polynomial $f_i(x)\in\mathbb{F}_q[x]$. Thirdly, t could be even if n is odd because it is only required that $(t,(3^n-1)/2)=1$ in stead of $(t,3^n-1)=1$. For example, plug $t=2^i$ and $\theta=\beta=\alpha=1$ in Theorem 2.6 for $\mathbb{F}_{3^n}$ where n is odd, we obtain

Theorem 2.11. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+2^i}+2x^{\frac{3^n-1}{2}+3}+2x^{\frac{3^n-1}{2}+2}+2x^{\frac{3^n-1}{2}+1}+x^{2^i}+x^3+x^2+x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

In particular, when $i=1$, we have

Corollary 2.12. *The polynomial $f(x)=x^{\frac{3^n-1}{2}+3}+x^{\frac{3^n-1}{2}+1}+2x^3+x^2+2x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n.*

In a similar way, we obtain the following result which extends the previous results.

Theorem 2.13. *Let $q=3^n$ and t be any positive integer. Let $\alpha,\beta,\theta\in\mathbb{F}_q^*$ and*

$$f(x)=\begin{cases}0, & if\ x=0;\\ \beta(x^3+\theta x^2+\theta^2x), & if\ x\in C_0;\\ \alpha x^t, & if\ x\in C_1.\end{cases}$$

Then f is a PP of $\mathbb{F}_q$ if and only if $(t, \frac{q-1}{2}) = 1$, $\eta(\theta) = -1$, and any one of the following holds: (i) t is odd and $\eta(\alpha) = \eta(\beta)$; (ii) t is even and $\eta(\alpha) = -\eta(\beta)$. In this case, $f(x) = -(\beta x^3 + \beta\theta x^2 + \beta\theta^2 x - \alpha x^t)x^{\frac{3^n-1}{2}} - (\beta x^3 + \beta\theta x^2 + \beta\theta^2 x + \alpha x^t)$.

Proof. Assume f is a PP. Obviously, $(t, \frac{q-1}{2}) = 1$ because x^t maps C_0 onto either C_0 or C_1. Moreover, let $\beta(x^3 + \theta x^2 + \theta^2 x) = \beta(y^3 + \theta y^2 + \theta^2 y)$ for $x, y \in C_0$. Then we obtain $(x-y)(x^2 + (y-2\theta)x + (y-\theta)^2) = 0$. It is obvious that $(x^2 + (y-2\theta)x + (y-\theta)^2) = 0$ if and only if $\eta((y-2\theta)^2 - 4(y-\theta)^2) = \eta(\theta y) = 1$. Hence $\beta(x^3 + \theta x^2 + \theta^2 x)$ is one-to-one over C_0 if and only if $(x^2 + (y-2\theta)x + (y-\theta)^2) \neq 0$ over C_0. The latter is equivalent to $\eta(\theta y) \neq 1$ and thus $\eta(\theta) = -1$. We now consider two cases of t. If t is odd, then x^t maps C_1 onto C_1. Because $\beta(x^3 + \theta x^2 + \theta^2 x) = \beta x(x-\theta)^2$, we must have $\eta(\alpha) = \eta(\beta)$. If t is even, then x^t maps C_1 onto C_0. Because $(x^3 + \theta x^2 + \theta^2 x) = x(x-\theta)^2$ maps C_0 onto C_0, we must have $\eta(\alpha) = -\eta(\beta)$. The converse is similar and we omit the proof. □

For $t = 3^i$, $\theta = 2$, and $\alpha = \beta = 1$, we apply Theorem 2.13 over $\mathbb{F}_{3^n}$ with odd n to obtain the following result.

Theorem 2.14. *The polynomial $f(x) = x^{\frac{3^n-1}{2}+3^i} + 2x^{\frac{3^n-1}{2}+3} + x^{\frac{3^n-1}{2}+2} + 2x^{\frac{3^n-1}{2}+1} + 2x^{2^i} + 2x^3 + x^2 + 2x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

For $t = 2$, $\theta = \beta = 2$, and $\alpha = 1$, we apply Theorem 2.13 over $\mathbb{F}_{3^n}$ with odd n to obtain the following result.

Theorem 2.15. *The polynomial $f(x) = x^{\frac{3^n-1}{2}+2^i} + x^{\frac{3^n-1}{2}+3} + 2x^{\frac{3^n-1}{2}+2} + x^{\frac{3^n-1}{2}+1} + 2x^{2^i} + x^3 + 2x^2 + x$ is a PP of $\mathbb{F}_{3^n}$ for any odd positive integer n and non-negative integer i.*

In particular, when $i = 1$, we obtain

Theorem 2.16. *The polynomial $f(x) = x^{\frac{3^n-1}{2}+3} + x^{\frac{3^n-1}{2}+1} + x^3 + x^2 + x$ is a PP over $\mathbb{F}_{3^n}$ for any odd positive integer n.*

We also obtain the following PPs such that both branches are cubic polynomials.

Theorem 2.17. *Let $q = 3^n$ and $\alpha, \beta, \gamma, \theta \in \mathbb{F}_{3^n}$. Let $f(x) = (\beta - \alpha)x^{(q-1)/2+3} + (\beta\theta - \alpha\gamma)x^{(q-1)/2+2} + (\beta\theta^2 - \alpha\gamma^2)x^{(q-1)/2+1} - (\beta + \alpha)x^3 - (\beta\theta + \alpha\gamma)x^2 - (\beta\theta^2 + \alpha\gamma^2)x$. Then f is a PP of $\mathbb{F}_{3^n}$ if and only if $\eta(\alpha) = \eta(\beta)$, $\eta(\gamma) = -1$, and $\eta(\theta) = 1$.*

Proof. Obviously, we have

$$f(x) = \begin{cases} 0, & if\ x = 0; \\ \alpha(x^3 + \gamma x^2 + \gamma^2 x), & if\ x \in C_0; \\ \beta(x^3 + \theta x^2 + \theta^2 x), & if\ x \in C_1. \end{cases}$$

Assume f is a PP of $\mathbb{F}_q$. Because $\alpha(x^3 + \gamma x^2 + \gamma^2 x) = \alpha x(x-\gamma)^2$ and $\beta(x^3 + \theta x^2 + \theta^2 x) = \beta x(x-\theta)^2$, they map C_0 and C_1 into different cosets respectively, as long as $\eta(\alpha) = \eta(\beta)$.

Moreover, let $\beta(x^3+\theta x^2+\theta^2 x)=\beta(y^3+\theta y^2+\theta^2 y)$ with $x,y\in C_1$. Then we obtain $(x-y)(x^2+(y-2\theta)x+(y-\theta)^2)=0$. It is obvious that $(x^2+(y-2\theta)x+(y-\theta)^2)=0$ if and only if $\eta((y-2\theta)^2-4(y-\theta)^2)=\eta(\theta y)=1$. Hence $\beta(x^3+\theta x^2+\theta^2 x)$ is one-to-one over C_1 if and only if $\eta(\theta)=1$. Similarly, $\alpha(x^3+\gamma x^2+\gamma^2 x)$ is one to one over C_0 if and only if $\eta(\gamma)=-1$. □

For the rest of paper, we concentrate on refinement of Lemma 2.1 with more branches. Obviously, $A_i\neq 0$ for all i's if f is a PP. Moreover, if $r_i(x)$'s are of certain special formats then we can simplify Lemma 2.1 significantly.

One of the most natural choice is that $r_i(x)=x^{r_i}$ for $i=0,\ldots,\ell-1$. In this case, we must have $(r_i,s)=1$ in order for $P(x)$ to be a PP; otherwise, $|C_i^{r_i}|\neq s$, a contradiction. Hence we have the following result.

Theorem 2.18. *Let $\ell,s,r_0,\ldots,r_{\ell-1}$ be positive integers such that $s=(q-1)/\ell$ and $(r_i,s)=1$ for any $i=0,\ldots,\ell-1$. Let q be prime power and $A_0,\ldots,A_{\ell-1}\in\mathbb{F}_q^*$. Let*

$$P(x)=f_{A_0,A_1,\cdots,A_{\ell-1}}^{x^{r_0},x^{r_1},\ldots,x^{r_{\ell-1}}}(x)=\begin{cases}0, & if\ x=0;\\ A_0x^{r_0}, & if\ x\in C_0;\\ \vdots & \vdots\\ A_ix^{r_i}, & if\ x\in C_i;\\ \vdots & \vdots\\ A_{\ell-1}x^{r_{\ell-1}}, & if\ x\in C_{\ell-1}.\end{cases}$$

Then the following are equivalent.

(a) *$P(x)$ is a PP of $\mathbb{F}_q$;*
(b) *$A_iC_{ir_i}\neq A_{i'}C_{i'r_{i'}}$ for any $0\le i<i'\le \ell-1$, where the subscripts of C_{ir_i} are taken modulo ℓ.*
(c) *$Ind_\gamma(\frac{A_i}{A_{i'}})\not\equiv r_{i'}i'-r_ii \pmod{\ell}$ for any $0\le i<i'\le\ell-1$, where $ind_\gamma(a)$ is residue class $b \bmod q-1$ such that $a=\gamma^b$.*
(d) *$\{A_0,A_1\gamma^{r_i},\cdots,A_{\ell-1}\gamma^{(\ell-1)r_i}\}$ is a system of distinct representatives of $\mathbb{F}_q^*/C_0$.*
(e) *$\{A_i^s\zeta^{ir_i}\mid i=0,\cdots,\ell-1\}$ is the set μ_ℓ of all distinct ℓ-th roots of unity.*
(f) *$\sum_{i=0}^{\ell-1}\zeta^{cr_ii}A_i^{cs}=0$ for all $c=1,\cdots,\ell-1$.*

Proof. The proof is similar to the proof of Theorem 1 in [17] and we include it for the sake of completeness.

Since $C_i=\{\gamma^{\ell j+i}: j=0,1,\cdots,s-1\}$, for any two elements $x\neq y\in C_i$, we have $x=\gamma^{\ell j+i}$ and $y=\gamma^{\ell j'+i}$ for some $0\le j\neq j'\le s-1$. Since $(r_i,s)=1$, we obtain $A_ix^{r_i}=A_i\gamma^{\ell r_ij+ir_i}\neq A_iy^{r_i}=A_i\gamma^{\ell r_ij'+ir_i}$. Moreover, it is easy to prove that $C_0^{r_0}=C_0$ and more generally $C_i^{r_i}=C_{ir_i}$ for any $0\le i\le\ell-1$. Hence (a) and (b) are equivalent.

Because $A_i\gamma^{ir_i}$ is a coset representative of $A_iC_{ir_i}$, it is easy to see that (c), (d), and (e) are equivalent. Finally, since all of $A_0^s,A_1^s\zeta^{r_1},\cdots,A_{\ell-1}^s\zeta^{(\ell-1)r_{\ell-1}}$ are ℓ-th roots of

unity, (e) means that A_0^s, $A_1^s\zeta^{r_1}$, $\cdots$, $A_{\ell-1}^s\zeta^{(\ell-1)r_{\ell-1}}$ are all distinct. By Lemma 2.1 in [6], (e) is equivalent to (f). □

This result generalizes Theorem 2.2 [6], Theorem 1 [17], and Lemma 2.1 [21], and all the consequences in these references. Furthermore, we obtain the following result in terms of the polynomial presentation.

Theorem 2.19. *Let q be a prime power, $\ell \mid q-1$ and $s=(q-1)/\ell$. Let $\mathbb{F}_q$ be a finite field of q elements and $\zeta \in \mathbb{F}_q$ be a primitive ℓ-th root of unity. Let $A_0,\ldots,A_{\ell-1} \in \mathbb{F}_q^*$. Then*

$$P(x)=\sum_{i=0}^{\ell-1}\frac{A_i x^{r_i}}{\ell\zeta^{i(\ell-1)}}\left(x^{(\ell-1)s}+\zeta^i x^{(\ell-2)s}+\cdots+\zeta^{i(\ell-2)}x^s+\zeta^{i(\ell-1)}\right)$$

is a PP of $\mathbb{F}_q$ if and only if $(r_i,s)=1$ for all $i=0,\ldots,\ell-1$ and $\{A_i^s\zeta^{ir_i} \mid i=0,\cdots,\ell-1\}=\mu_\ell$, where μ_ℓ is the set of all ℓ-th roots of unity. The latter condition is equivalent to that $\{t_i+ir_i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ, where $A_i^s=\zeta^{t_i}$ for $i=0,\ldots,\ell-1$. In particular, if $A_0^s=A_1^s=\ldots=A_{\ell-1}^s\neq 0$, then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r_i,s)=1$ for all $i=0,\ldots,\ell-1$ and $\{ir_i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ.

Proof. By Theorem 2.18 and Equation (1), $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r_i,s)=1$ for all $i=0,\ldots,\ell-1$ and $\{A_i^s\zeta^{ir_i} \mid i=0,\cdots,\ell-1\}$ is the set μ_ℓ of all distinct ℓ-th roots of unity. Moreover, $\{A_i^s\zeta^{ir_i}=\zeta^{t_i+ir_i} \mid i=0,\cdots,\ell-1\}=\mu_\ell$ is equivalent to that $\{t_i+ir_i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ. □

Theorem 2.19 provides a simple algorithmic way to construct PPs of $\mathbb{F}_q$ with large indices. First, take any factor ℓ of $q-1$ and let $s=\frac{q-1}{\ell}$. Then pick any ℓ positive integers $r_0,\ldots,r_{\ell-1}$ such that $(r_i,s)=1$ for $i=0,\ldots,\ell-1$ and any ℓ nonzero constants $A_0,\ldots,A_{\ell-1}\in\mathbb{F}_q^*$. As long as $A_i^s\zeta^{ir_i}$ $(0\le i\le \ell-1)$ are all distinct (equivalently, $\{t_i+ir_i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ), we obtain a PP of $\mathbb{F}_q$. In this way, one can construct a very large amount of classes of PPs of $\mathbb{F}_q$. Here we give a few more examples of PPs of finite fields produced by our construction method.

First we consider a few classes of PPs with three branches.

Corollary 2.20. *Let $q=p^n$ such that $3 \mid q-1$ and $s=\frac{q-1}{3}$. Let ζ be a primitive 3-rd root of unity. Let $A_0,A_1,A_2\in\mathbb{F}_q$. Then $P(x)=A_0x^{r_0}\left(x^{2s}+x^s+1\right)+\zeta A_1x^{r_1}\left(x^{2s}+\zeta x^s+\zeta^2\right)+\zeta^2A_2x^{r_2}\left(x^{2s}+\zeta^2x^s+\zeta\right)$ is a PP of $\mathbb{F}_q$ if and only if $(r_i,s)=1$ for $i=0,1,2$ and $\{A_0^s,A_1^s\zeta^{r_1},A_2^s\zeta^{2r_2}\}=\{1,\zeta,\zeta^2\}$.*

The following result generalizes Theorem 9 in [20]. Again, we show these conditions are both necessary and sufficient.

Theorem 2.21. *Assume $p^n\equiv 1 \pmod 3$. Let $s=\frac{p^n-1}{3}$ and ζ be an element of $\mathbb{F}_{p^n}$ of order 3. Then*

$$f(x)=x(x^s-\zeta)(x^s-\zeta^2)+x^3(x^s-1)(x^s-\zeta^2)+\zeta x^p(x^s-1)(x^s-\zeta)$$

is a PP over $\mathbb{F}_{p^n}$ if and only if

(a) $p \equiv 1 \pmod 3$ and $s \equiv 1 \pmod 3$; or

(b) $p \equiv 2 \pmod 3$ and $s \equiv 2 \pmod 3$.

Proof. In this case, $\ell = 3$ and $r_0 = 1, r_1 = 3, r_2 = p$. Also $f_0(x) = (x-\zeta)(x-\zeta^2)$, $f_1(x) = (x-1)(x-\zeta^2)$, and $f_2(x) = \zeta(x-1)(x-\zeta)$. So $A_0 = (1-\zeta)(1-\zeta^2) = 1-\zeta-\zeta^2+\zeta^3 = 2-\zeta-\zeta^2 = 3$, $A_1 = (\zeta-1)(\zeta-\zeta^2) = 3\zeta^2$, and $A_2 = \zeta(\zeta^2-1)(\zeta^2-\zeta) = 3\zeta^2$. Hence

$$f(x) = f_{A_0,A_1,A_2}^{x^1,x^3,x^p}(x) = \begin{cases} 0 & x = 0; \\ 3x & x \in C_0; \\ 3\zeta^2 x^3 & x \in C_1; \\ 3\zeta^2 x^p & x \in C_2. \end{cases}$$

Obviously, we have $(r_i, s) = 1$ for $i = 0, 1, 2$. Moreover, $\{A_0^s, A_1^s\zeta^3, A_2^s\zeta^{2p}\} = \{3^s, 3^s\zeta^{2s+3}, 3^s\zeta^{2s+2p}\}$ is equal to $\{1, \zeta^{2s}, \zeta^{2s+2p}\}$ if and only if p, s satisfy either $p \equiv 1 \pmod 3$ and $s \equiv 1 \pmod 3$, or $p \equiv 2 \pmod 3$ and $s \equiv 2 \pmod 3$. By Corollary 2.20, we complete our proof. □

The following result also generalizes Theorem 10 in [20].

Theorem 2.22. *Let i be any positive integer and assume $p^n \equiv 1 \pmod 9$. Let $s = \frac{p^n-1}{3}$ and ζ be an element of $\mathbb{F}_{p^n}$ of order 3. Then*

$$f(x) = x(x^s-\zeta)(x^s-\zeta^2) + x^{p^i}(x^s-1)(x^s-\zeta^2) + \zeta x^p(x^s-1)(x^s-\zeta)$$

is a PP over $\mathbb{F}_{p^n}$ if and only if

(i) $p \equiv 1 \pmod 3$; or

(ii) i is odd and $p \equiv 2 \pmod 3$.

Proof. In this case, $\ell = 3$ and $r_0 = 1, r_1 = p^i, r_2 = p$. Also $f_0(x) = (x-\zeta)(x-\zeta^2)$, $f_1(x) = (x-1)(x-\zeta^2)$, and $f_2(x) = \zeta(x-1)(x-\zeta)$. So $A_0 = (1-\zeta)(1-\zeta^2) = 1-\zeta-\zeta^2+\zeta^3 = 2-\zeta-\zeta^2 = 3$, $A_1 = (\zeta-1)(\zeta-\zeta^2) = 3\zeta^2$, and $A_2 = \zeta(\zeta^2-1)(\zeta^2-\zeta) = 3\zeta^2$. Hence

$$f(x) = f_{A_0,A_1,A_2}^{x^1,x^{p^i},x^p}(x) = \begin{cases} 0 & x = 0; \\ 3x & x \in C_0; \\ 3\zeta^2 x^{p^i} & x \in C_1; \\ 3\zeta^2 x^p & x \in C_2. \end{cases}$$

Obviously, we have $(r_j, s) = 1$ for $j = 0, 1, 2$. Therefore, by Corollary 2.20, $f(x)$ is a PP over $\mathbb{F}_q$ if and only if $\{A_j^s\zeta^{r_j j} \mid j = 0, 1, 2\} = \{1, \zeta, \zeta^2\}$. Indeed, $\{A_j^s\zeta^{r_j j} \mid j = 0, 1, 2\} = \{3^s, (3\zeta^2)^s\zeta^{p^i}, (3\zeta^2)^s\zeta^{2p}\}$. We only need to find conditions so that $1, \zeta^{2s+p^i}, \zeta^{2s+2p}$ are all distinct, equivalently, $2s+p^i \not\equiv 0 \pmod 3$, $s+p \not\equiv 0 \pmod 3$ and $2s+p^i \not\equiv 2s+2p \pmod 3$. Under the assumption of $p^n \equiv 1 \pmod 9$, we have $s \equiv 0 \pmod 3$. Hence we require $p^i \not\equiv 0 \pmod 3$, $p \not\equiv 0 \pmod 3$ and $p^i \not\equiv 2p \pmod 3$. Therefore either $p \equiv 1 \pmod 3$, or $p \equiv 2 \pmod 3$ and i is odd. □

In particular, if A_0, A_1, A_2 belong to the same cyclotomic coset, then the condition $\{A_0^s, A_1^s\zeta^{r_1}, A_2^s\zeta^{2r_2}\} = \{1, \zeta, \zeta^2\}$ reduces $\{1, \zeta^{r_1}, \zeta^{2r_2}\} = \{1, \zeta, \zeta^2\}$, which is equivalent to $r_1 \equiv r_2 \not\equiv 0 \pmod 3$.

Corollary 2.23. *Let $q = p^n$ such that $3 \mid q-1$ and $s = \frac{q-1}{3}$. Let ζ be a primitive 3-rd root of unity. Let $A_0, A_1, A_2 \in \mathbb{F}_q$ such that $A_0^s = A_1^s = A_2^s$. Then $P(x) = A_0x^{r_0}(x^{2s} + x^s + 1) + A_1x^{r_1}\ (\zeta x^{2s} + \zeta^2 x^s + 1) + A_2x^{r_2}\left(\zeta^2 x^{2s} + \zeta x^s + 1\right)$ is a PP of $\mathbb{F}_q$ if and only if $(r_i, s) = 1$ for $i = 0, 1, 2$ and $r_1 \equiv r_2 \not\equiv 0 \pmod 3$.*

From this corollary, if we take $q = 2^n$ with n is even, $A_0 = A_1 = A_2 = 1$, $r_0 = 2^i$ and $r_1 = r_2 = 2^j$ for some non negative integers i, j, we obtain the following classes of PPs with coefficients in $\mathbb{F}_2$.

Theorem 2.24. *The polynomial $P(x) = x^{\frac{2(2^n-1)}{3}+2^i} + x^{\frac{2(2^n-1)}{3}+2^j} + x^{\frac{2^n-1}{3}+2^i} + x^{\frac{2^n-1}{3}+2^j} + x^{2^i}$ is a PP over $\mathbb{F}_{2^n}$ for any even positive integer n and non-negative integers i, j.*

Similarly, we can construct PPs with coefficients in general base field $\mathbb{F}_p$.

Theorem 2.25. *Let $q = p^m$, ℓ be a prime factor of $q-1$ with $s = \frac{q-1}{\ell}$. Let $A_0, A_1 \in \mathbb{F}_q^*$. Then $f(x) = A_0x^{r_0}\left(x^{(\ell-1)s} + \cdots + x^s + 1\right) - A_1x^{r_1}\left(x^{(\ell-1)s} + \cdots + x^s + \ell - 1\right)$ is a PP of $\mathbb{F}_q$ if and only if $(r_0, s) = (r_1, s) = 1$ and $A_0^s = A_1^s$.*

Proof. Let $P(x)$ be the cyclotomic mapping $f^{r_0,r_1,\ldots,r_1}_{A_0,A_1,\ldots,A_1}(x)$, we obtain

$$\begin{aligned}
P(x) &= \frac{A_0x^{r_0}}{\ell}\left(x^{(\ell-1)s} + x^{(\ell-2)s} + \cdots + x^s + 1\right) \\
&\quad + \sum_{i=1}^{\ell-1} \frac{A_ix^{r_i}}{\ell\zeta^{i(\ell-1)}}\left(x^{(\ell-1)s} + \zeta^i x^{(\ell-2)s} + \cdots + \zeta^{i(\ell-2)}x^s + \zeta^{i(\ell-1)}\right) \\
&= \frac{A_0x^{r_0}}{\ell}\left(x^{(\ell-1)s} + x^{(\ell-2)s} + \cdots + x^s + 1\right) \\
&\quad + \frac{A_1x^{r_1}}{\ell}\left(\sum_{i=1}^{\ell-1}\zeta^{-i(\ell-1)}x^{(\ell-1)s} + \sum_{i=1}^{\ell-1}\zeta^{-i(\ell-2)}x^{(\ell-2)s} + \cdots + \sum_{i=1}^{\ell-1}\zeta^{-i}x^s + \ell - 1\right) \\
&= \frac{A_0x^{r_0}}{\ell}\left(x^{(\ell-1)s} + x^{(\ell-2)s} + \cdots + x^s + 1\right) - \frac{A_1x^{r_1}}{\ell}\left(x^{(\ell-1)s} + \cdots + x^s + \ell - 1\right),
\end{aligned}$$

where the last equality holds because $\sum_{i=1}^{\ell-1}\zeta^{-i(\ell-j)} = -1$ for all $j = 1, \ldots, \ell-1$ when ℓ is prime. By Theorem 2.19 and let $r_1 = \cdots = r_{\ell-1}$ and $A_1 = \cdots = A_{\ell-1}$, $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r_0, s) = (r_1, s) = 1$ and $\{A_0^s, A_1^s\zeta^{r_1}, \ldots, A_1^s\zeta^{(\ell-1)r_1}\} = \mu_\ell$. The latter condition is equivalent to $A_0^s \neq A_1^s\zeta^{ir_1}$ for all $i = 1, \ldots, \ell-1$, namely, $A_1^s = A_0^s$. □

Taking $A_0 = A_1 = 1$, we obtain the following PP with coefficients in the prime field $\mathbb{F}_p$.

Corollary 2.26. *Let $q = p^m$, ℓ be a prime factor of $q-1$ with $s = \frac{q-1}{\ell}$. Then $f(x) = x^{r_0}\left(x^{(\ell-1)s} + \cdots + x^s + 1\right) - x^{r_1}\left(x^{(\ell-1)s} + \cdots + x^s + \ell - 1\right)$ is a PP of $\mathbb{F}_q$ if and only if $(r_0, s) = (r_1, s) = 1$.*

Finally we give another application of Theorem 2.19, which generalizes Theorem 11 in [20].

Theorem 2.27. *Assume $p^n \equiv 1 \pmod{\ell^2}$ and let θ be an element of $\mathbb{F}_{p^n}$ of order ℓ. Then*

$$f(x) = \sum_{i=1}^{t} x^{p^i} \prod_{j=1, j\neq i}^{t} (x^{(p^n-1)/\ell} - \theta^j)$$

is a PP over $\mathbb{F}_{p^n}$ if and only if $\{ip^i \pmod{\ell} \mid i = 0, \ldots, \ell-1\} = \mathbb{Z}_\ell$.

Proof. Let $s = \frac{p^n-1}{\ell}$. We note that f is a cyclotomic mapping with $r_i = p^i$ for $i = 0, \ldots, \ell-1$ and $A_i = \prod_{j=1, j\neq i}^{t}(\theta^i - \theta^j) = \theta^{i(\ell-1)}(1-\theta^{-1})\cdots(1-\theta^{-(\ell-1)}) = \ell\theta^{i(\ell-1)}$. By Theorem 2.19, f is a PP of $\mathbb{F}_q$ if and only if $(p^i, q-1) = 1$ for all $i = 0, \ldots, \ell-1$ and $\{\ell^s\theta^{i(\ell-1)s}\theta^{ip^i} \mid i = 0, \ldots, \ell-1\} = \mu_\ell$. The condition $p^n \equiv 1 \pmod{\ell^2}$ implies $\ell \mid s$ and thus $\theta^{i(\ell-1)s} = 1$. Hence $\{\ell^s\theta^{ip^i} \mid i = 0, \ldots, \ell-1\} = \mu_\ell$ if and only if $\{ip^i \pmod{\ell} \mid i = 0, \ldots, \ell-1\} = \mathbb{Z}_\ell$. □

Corollary 2.28 (Theorem 11, [20])**.** *Assume $p \equiv 1 \pmod{\ell}$ and $p^n \equiv 1 \pmod{\ell^2}$ and let θ be an element of $\mathbb{F}_{p^n}$ of order ℓ. Then*

$$f(x) = \sum_{i=1}^{t} x^{p^i} \prod_{j=1, j\neq i}^{t} (x^{(p^n-1)/\ell} - \theta^j)$$

is a PP over $\mathbb{F}_{p^n}$

Corollary 2.29. *Assume $p^n \equiv 1 \pmod{16}$ and let θ be an element of $\mathbb{F}_{p^n}$ of order ℓ. Then*

$$f(x) = \sum_{i=1}^{t} x^{p^i} \prod_{j=1, j\neq i}^{t} (x^{(p^n-1)/\ell} - \theta^j)$$

is a PP over $\mathbb{F}_{p^n}$.

Proof. Obviously, p must be odd. If $p \equiv 1 \pmod{4}$, then f is PP over $\mathbb{F}_{p^n}$ by Corollary 2.28. If $p \equiv 3 \pmod{4}$, then $\{ip^i \mid i = 0, 1, 2, 3\} = \{0, p, 2p^2, 3p^3\}$ is indeed a complete set of residue modulo 4. By Theorem 2.27, f is a PP over $\mathbb{F}_{p^n}$. □

Similarly, we obtain the following corollary.

Corollary 2.30. *Assume $p^n \equiv 1 \pmod{25}$ and let θ be an element of $\mathbb{F}_{p^n}$ of order ℓ. Then*

$$f(x) = \sum_{i=1}^{t} x^{p^i} \prod_{j=1, j\neq i}^{t} (x^{(p^n-1)/\ell} - \theta^j)$$

is a PP over $\mathbb{F}_{p^n}$ if and only if $p \equiv 1 \pmod{5}$.

3. Realization of constants by polynomials

In this section, we give more applications of Theorem 2.18 (or another version as in Theorem 3.1) to construct many new classes of PPs which have large indices and simple descriptions. We mainly consider how to choose constants $A_0, \ldots, A_{\ell-1}$ in terms of polynomials of specific formats in the cyclotomic mappings constructions. This demonstrate that our results generalize these results in [1, 5, 6, 21].

First of all, another way to rewrite Theorem 2.18 is as follow:

Theorem 3.1. *Let $q-1=\ell s$, $f_0(x), \ldots, f_{\ell-1}(x) \in \mathbb{F}_q[x]$ and*

$$P(x)=\begin{cases} 0, & if\ x=0;\\ x^{r_0}f_0(x^s), & if\ x\in C_0;\\ x^{r_1}f_1(x^s), & if\ x\in C_1;\\ \vdots & \vdots\\ x^{r_{\ell-1}}f_{\ell-1}(x^s), & if\ x\in C_\ell. \end{cases}$$

Then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r_i, s)=1$ for any $i=0,1,\ldots,\ell-1$ and $\mu_\ell=\{\zeta^{r_i i}f_i(\zeta^i)^s \mid i=0,\ldots,\ell-1\}$, where μ_ℓ is the set of all ℓ-th roots of unity.

Using Equation (1) and Theorem 3.1, we can construct many PPs in the following polynomial format with large indices.

$$P(x)=\sum_{i=0}^{\ell-1}\frac{x^{r_i}f_i(x^s)}{\ell\zeta^{i(\ell-1)}}\left(x^{(\ell-1)s}+\zeta^i x^{(\ell-2)s}+\cdots+\zeta^{i(\ell-2)}x^s+\zeta^{i(\ell-1)}\right). \tag{2}$$

As long as $f_i(\zeta^i)\neq 0$, we can rewrite Theorem 3.1 as follow:

Theorem 3.2. *Let $q-1=\ell s$, $f_1(x), \ldots, f_{\ell-1}(x) \in \mathbb{F}_q[x]$, and*

$$P(x)=\begin{cases} 0, & if\ x=0;\\ x^{r_0}f_0(x^s), & if\ x\in C_0;\\ x^{r_1}f_1(x^s), & if\ x\in C_1;\\ \vdots & \vdots\\ x^{r_{\ell-1}}f_{\ell-1}(x^s), & if\ x\in C_\ell. \end{cases}$$

Suppose $f_i(\zeta^i)^s=A\zeta^{n_i}$ for each $i=0,\ldots,\ell-1$ and a nonzero constant $A\in\mathbb{F}_q^*$. Then $P(x)$ is a PP of $\mathbb{F}_q$ if and only if

(i) *$(r_i, s)=1$ for any $i=0,\ldots,\ell-1$.*

(ii) *$\{ir_i+n_i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ.*

In particular, if $f_i(\zeta^i)^s=A$ for each $i=0,\ldots,\ell-1$ and a nonzero constant $A\in\mathbb{F}_q^*$, then P is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r_i, s)=1$ for $i=0,\ldots,\ell-1$ and $\{r_i i \mid i=0,\ldots,\ell-1\}$ is a complete set of residues modulo ℓ.

Proof. Because the constant A appears in each branch of the definition of $P(x)$, we can assume $A=1$ without loss of generality. From Theorem 3.1, we need to show that

condition (ii) is equivalent to that $\mu_\ell = \{\zeta^{r_i i} f_i(\zeta^i)^s = \zeta^{ir_i+n_i} \mid i = 0, \ldots, \ell-1\}$, which is obvious. □

We note that if $r_0 = r_1 = \cdots = r_{\ell-1} := r$, then $\{r_i i \mid i = 0, \ldots, \ell-1\}$ is a complete set of residues modulo ℓ if and only if $(r, \ell) = 1$. If $r_0 = \cdots = r_{\ell-1}$ and $n_0 = \cdots = n_{\ell-1}$, we obtain Theorem 4.1 in [6] as a corollary. As a special case of Theorem 3.2, we also have the following result.

Corollary 3.3. *Let $q-1 = \ell s$, $g_1(x), \ldots, g_{\ell-1}(x)$ be any ℓ polynomials over $\mathbb{F}_q$, and*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{r_0} g_0(x^s)^\ell, & if\ x \in C_0; \\ x^{r_1} g_1(x^s)^\ell, & if\ x \in C_1; \\ \vdots & \vdots \\ x^{r_{\ell-1}} g_{\ell-1}(x^s)^\ell, & if\ x \in C_\ell. \end{cases}$$

Then $P(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\{r_i i \mid i = 0, \ldots, \ell-1\}$ is a complete set of residues modulo ℓ, $(r_i, s) = 1$ and $g_i(\zeta^i) \neq 0$ for all $0 \leq i \leq \ell-1$.

Proof. This is true since if we set $f_i(x) = g_i(x)^\ell$, then we have $f_i(\zeta^i)^s = g_i(\zeta^i)^{\ell s} = g_i(\zeta^i)^{q-1} = 1$. The result follows from Theorem 3.2. □

We note that earlier results of Wan and Lidl (see Corollary 1.4 in [16]), and Akbary and Wang (Theorem 3.1 in [6]) are also special cases of the above result.

We next construct cyclotomic permutations using classes of PPs with coefficients in some appropriate subfield which has been studied in [1], [5], [6], [7], and [21].

Theorem 3.4. *Let $\ell, r_0, \ldots, r_{\ell-1}$ be a positive integer with $q-1 = \ell s$. Suppose $q = q_0^m$ where $q_0 \equiv 1 \pmod{\ell}$ and $\ell \mid m$. Let $f_1(x), \ldots, f_{\ell-1}(x)$ be polynomials in $\mathbb{F}_{q_0}[x]$ and*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{r_0} f_0(x^s), & if\ x \in C_0; \\ x^{r_1} f_1(x^s), & if\ x \in C_1; \\ \vdots & \vdots \\ x^{r_{\ell-1}} f_{\ell-1}(x^s), & if\ x \in C_\ell. \end{cases}$$

Then the polynomial $P(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\{r_i i \mid i = 0, \ldots, \ell-1\}$ is a complete set of residues modulo ℓ, $(r_i, s) = 1$ and $f_i(\zeta^i) \neq 0$ for all $0 \leq i \leq \ell-1$.

Proof. Let $m = \ell n$. The result is clear from Theorem 3.2, since we have

$$\begin{aligned} f_i(\zeta^i)^{\frac{q-1}{\ell}} &= f_i(\zeta^i)^{\frac{q_0^{\ell n}-1}{\ell}} \\ &= f_i(\zeta^i)^{\frac{q_0^n-1}{\ell}\left((q_0^n)^{\ell-1}+(q_0^n)^{\ell-2}+\cdots+1\right)} \\ &= \left(\prod_{j=0}^{\ell-1} f_i(\zeta^i)^{q_0^{nj}}\right)^{\frac{q_0^n-1}{\ell}} \\ &= \left(f_i(\zeta^i)^{\ell}\right)^{\frac{q_0^n-1}{\ell}} \\ &= 1. \end{aligned}$$

□

For example, let v be the order of p in $\mathbb{Z}/\ell\mathbb{Z}$. For any positive integer n, we can take $q = q_0^m = p^{\ell v n}$ in the above result. We note Theorem 3.4 generalizes Corollary 3.3 ([6] or Theorem 3.1 ([7]) or Theorem 1.2 ([21]), which deal with the case $P(x) = x^r f(x^s)$.

Moreover, in [1, 6, 21], classes of PPs of the form $x^r(1+x^{e_1 s}+\ldots+x^{e_k s})^t$ are studied. For $h(x) = 1 + x + \cdots + x^k$, it is well known that $h(\zeta^0) = k + 1 \neq 0$ if and only if $p \nmid (k+1)$ and $h(\zeta^i) = \frac{\zeta^{(k+1)i}-1}{\zeta^i-1} \neq 0$ if and only if $\ell \nmid (k+1)i$ for $i = 1, \ldots, \ell-1$. Here we construct cyclotomic permutations from these classes which generalizes Theorem 5.2 ([1]) and Corollary 2.3 ([21]).

Corollary 3.5. *Let ℓ be positive integer with $q - 1 = \ell s$. For all $i = 0, \ldots, \ell - 1$, let r_i, k_i, e_i, t_i be positive integers such that $(\ell, e_i) = 1$ and $h_{k_i}(x) = 1 + x + \cdots + x^{k_i}$. Suppose $q = q_0^m \pmod{\ell}$ such that $q_0 \equiv 1 \pmod{\ell}$ and $\ell \mid m$. Then*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{r_0} h_{k_0}(x^{e_0 s})^{t_0}, & if\ x \in C_0; \\ x^{r_1} h_{k_1}(x^{e_1 s})^{t_1}, & if\ x \in C_1; \\ \vdots & \vdots \\ x^{r_{\ell-1}} h_{k_{\ell-1}}(x^{e_{\ell-1} s})^{t_{\ell-1}}, & if\ x \in C_\ell, \end{cases}$$

permutes $\mathbb{F}_q$ if and only if $\{r_i i \mid i = 0, \ldots, \ell - 1\}$ is a complete set of residues modulo ℓ, $(r_i, s) = 1$ for all $0 \leq i \leq \ell - 1$, $p \nmid k_0 + 1$, and $\ell \nmid i(k_i + 1)$ for all $i = 1, \ldots, \ell - 1$.

Now we construct several classes of PPs obtained from Theorem 3.2 such that $f_i(\zeta^i)^s$ $(i = 0, \ldots, \ell - 1)$ are not necessarily the same. Again, the following result extends Theorem 4.4 in [6] and Theorem 1.3 in [21].

Theorem 3.6. *Let ℓ be positive integer with $q - 1 = \ell s$. For all $i = 0, \ldots, \ell - 1$, let r_i, k_i, e_i, t_i, n_i be positive integers such that $(\ell, e_i) = 1$. Put $h_{k_i'}(x) = 1 + x + \cdots + x^{k_i'}$ and $h_{k_i}(x) = 1 + x + \cdots + x^{k_i}$. Let $\bar{k_i} = \ell/(\ell, k_i)$. Suppose $q = q_0^m$ such that $q_0 \equiv -1$*

(mod ℓ) *and* m *is even. Pick* $\hat{h}_i \in \mathbb{F}_{q_0}[x]$ *and let* $f_i(x) := h_{k_i'}(x)^{t_i}\hat{h}_i(h_{k_i}(x)^{\bar{k_i}})$. *Then*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{r_0} f_0(x^{e_0 s}), & if\ x \in C_0; \\ x^{r_1} f_1(x^{e_1 s}), & if\ x \in C_1; \\ \vdots & \vdots \\ x^{r_{\ell-1}} f_{\ell-1}(x^{e_{\ell-1} s}), & if\ x \in C_\ell, \end{cases}$$

permutes $\mathbb{F}_q$ *if and only if* $\{(r_i + \frac{e_i k_i' t_i s}{2})i \mid i = 0, \ldots, \ell-1\}$ *is a complete set of residues modulo* ℓ, $(r_i, s) = 1$ *and* $f_i(\zeta^i) \neq 0$ *for all* $0 \leq i \leq \ell - 1$.

Proof. Let $m = 2n$. We note that $\ell \mid q_0 + 1$ implies that $\zeta^{q_0} = \zeta^{-1}$ and thus $h_{k_i'}(\zeta^{ie_i})^{q_0-1} = \left(\frac{\zeta^{(k_i'+1)ie_i q_0}-1}{\zeta^{ie_i q_0}-1}\right)\left(\frac{\zeta^{ie_i}-1}{\zeta^{(k_i'+1)ie_i}-1}\right) = \zeta^{-k_i' ie_i}$. Furthermore, $q_0 - 1 \mid \frac{q_0^2-1}{q_0+1} \mid \frac{q-1}{q_0+1} \mid \frac{q-1}{\ell} = s$ implies that $h_{k_i'}(\zeta^{ie_i})^s = \zeta^{-\frac{k_i' ie_i s}{q_0-1}} = \zeta^{\frac{k_i' ie_i s}{2}}$. Similarly, $h_{k_i}(\zeta^{ie_i})^{\bar{k_i} q_0} = \left(\frac{h_{k_i}(\zeta^{ie_i})}{\zeta^{k_i ie_i}}\right)^{\bar{k_i}} = h_{k_i}(\zeta^{ie_i})^{\bar{k_i}}$ implies that $h_{k_i}(\zeta^{ie_i})^{\bar{k_i}} \in \mathbb{F}_{q_0}$. Then the result follows from Theorem 3.2, since we have

$$\begin{aligned} f_i(\zeta^{ie_i})^{\frac{q-1}{\ell}} &= \left(h_{k_i'}(\zeta^{ie_i})^{t_i}\right)^{\frac{q-1}{\ell}} \left(\hat{h}_i(h_{k_i}(\zeta^{ie_i})^{\bar{k_i}})\right)^{\frac{q_0^{2n}-1}{\ell}} \\ &= h_{k_i'}(\zeta^{ie_i})^{t_i s} \left(\hat{h}_i(h_{k_i}(\zeta^{ie_i})^{\bar{k_i}})\right)^{\frac{q_0^2-1}{\ell}\left((q_0^2)^{n-1}+(q_0^2)^{n-2}+\cdots+1\right)} \\ &= \zeta^{\frac{ie_i k_i' t_i s}{2}} \left(\prod_{j=0}^{n-1} \hat{h}_i(h_{k_i}(\zeta^{ie_i})^{\bar{k_i}})^{q_0^{2j}}\right)^{\frac{q_0^2-1}{\ell}} \\ &= \zeta^{\frac{ie_i k_i' t_i s}{2}}, \end{aligned}$$

as long as $f_i(\zeta^{ie_i}) \neq 0$. □

Again, for $h(x) = 1 + x + \cdots + x^k$, it is well known that $h(\zeta^0) = k + 1 \neq 0$ if and only if $p \nmid (k+1)$ and that $h(\zeta^i) = \frac{\zeta^{(k+1)i}-1}{\zeta^i - 1} \neq 0$ if and only if $\ell \nmid (k+1)i$ for $i = 1, \ldots, \ell - 1$. We therefore obtain a generalization of Theorem 4.4 ([6]) and Corollary 2.4 ([21]) as follows:

Corollary 3.7. *Let* ℓ *be positive integer with* $q - 1 = \ell s$. *For all* $i = 0, \ldots, \ell - 1$, *let* r_i, k_i, e_i, t_i, n_i *be positive integers such that* $(\ell, e_i) = 1$. *Put* $h_{k_i}(x) = 1 + x + \cdots + x^{k_i}$. *Suppose* $q = q_0^m$ *such that* $q_0 \equiv -1$ (mod ℓ) *and* m *is even. Then*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{r_0} h_{k_0}(x^{e_0 s})^{t_0}, & if\ x \in C_0; \\ x^{r_1} h_{k_1}(x^{e_1 s})^{t_1}, & if\ x \in C_1; \\ \vdots & \vdots \\ x^{r_{\ell-1}} h_{k_{\ell-1}}(x^{e_{\ell-1} s})^{t_{\ell-1}}, & if\ x \in C_\ell, \end{cases}$$

permutes $\mathbb{F}_q$ *if and only if* $\{(r_i + \frac{e_i k_i t_i s}{2})i \mid i = 0, \ldots, \ell - 1\}$ *is a complete set of residue modulo* ℓ, $(r_i, s) = 1$ *for all* $0 \le i \le \ell - 1$, $p \nmid k_0 + 1$, *and* $\ell \nmid i(k_i + 1)$ *for all* $i = 1, \ldots, \ell - 1$.

Finally we take all branches as binomials and obtain a large class of PPs, which generalizes Theorem 3.1 [5] and Theorem 2.5 [21]. We note the necessary and sufficient description of a subclass of permutation binomials can be found in [17, 18].

Theorem 3.8. *Let* ℓ *be positive integer with* $q - 1 = \ell s$. *Let* $u_i > r_i > 0$ *and* $a_i \in \mathbb{F}_q^*$ *such that* $\gcd(u_i - r_i, q-1) := s$ *is a constant for all* $i = 0, \ldots, \ell - 1$. *Let* $e_i := (u_i - r_i)/\ell$ *and* η *be a fixed primitive* 2ℓ*-th root of unity in the algebraic closure of* $\mathbb{F}_q$ *and* $\zeta = \eta^2$. *Suppose* $(\eta^{ie_i} + a_i/\eta^{ie_i})^s = 1$ *for each* $i = 0, \ldots, \ell - 1$. *Then*

$$P(x) = \begin{cases} 0, & if\ x = 0; \\ x^{u_0} + a_0 x^{r_0}, & if\ x \in C_0; \\ x^{u_1} + a_1 x^{r_1}, & if\ x \in C_1; \\ \vdots & \vdots \\ x^{u_{\ell-1}} + a_{\ell-1} x^{r_{\ell-1}}, & if\ x \in C_\ell. \end{cases}$$

permutes $\mathbb{F}_q$ *if and only if* $-a_i \neq \zeta^{ie_i}$ *and* $(r_i, s) = 1$ *for all* $0 \le i \le \ell - 1$, $\{r_i i + \frac{e_i s i}{2} \mid i = 0, \ldots, \ell - 1\}$ *is a complete set of residues modulo* ℓ.

Proof. Let $x^{u_i} + a_i x^{r_i} = x^{r_i}(x^{e_i s} + a)$. We have

$$\begin{aligned} (\zeta^{ie_i} + a)^s &= (\eta^{2ie_i} + a)^s \\ &= \eta^{ie_i s} \left(\eta^{ie_i} + a/\eta^{ie_i}\right)^s \\ &= \eta^{ie_i s} = \zeta^{ie_i s/2}. \end{aligned}$$

The rest of proof follows easily from Theorem 3.2. □

4. CONCLUSION

In this paper we study permutation polynomials of finite fields in terms of cyclotomy. We provide both theoretical and algorithmic ways to generate permutation polynomials of finite fields. We have demonstrated how to construct concrete classes of PPs using our method. One can expect to generate more concrete classes of permutation polynomials by taking different polynomials as branches in our cyclotomic mapping construction. It is also expected to further extend our method to additive cyclotomy as studied in [3, 19, 23].

REFERENCES

[1] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory* **4** (2008), no. 1, 121-133.

[2] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* **15** (2009), 195-206.

[3] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* **17** (2011), no. 1, 51-67.

[4] A. Akbary and Q. Wang, On some permutation polynomials, *Int. J. Math. Math. Sci.* **16** (2005), 2631–2640.

[5] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.* **134** (2006), no 1, 15-22.

[6] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.*, Volume 2007, Article ID 23408, 7 pages.

[7] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* **13** (2007), 58-70.

[8] X. Hou, Two classes of permutation polynomials over finite fields, *J. Combin. Theory Ser A* **118** (2011), no. 2, 448-454.

[9] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, *Amer. Math. Monthly* **95** (1988), 243-246.

[10] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* **100** (1993), 71-74.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1997.

[12] G. L. Mullen, Permutation polynomials over finite fields, "Finite Fields, Coding Theory, and Advances in Communications and Computing", 131-151, Marcel Dekker, New York, 1993.

[13] G. L. Mullen and Q. Wang, Permutation polynomials of one variable, Section 8.1 in Handbook of Finite Fields, to appear.

[14] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc. Ser. A* **33** (1982) 197–212.

[15] H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, *Discrete Math.* **295** (2005), 161-171.

[16] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* **112** (1991), 149–163.

[17] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, Sequences, subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), *Lecture Notes in Comput. Sci.* 4893, 119–128.

[18] Q. Wang, On generalized Lucas sequences, Combinatorics and Graphs: the twentieth anniversary conference of IPM, May 15-21, 2009, *Contemporary Mathematics* **531** (2010), 127-141.

[19] P. Yuan and C. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.* **17** (2011), no. 6, 560 - 574.

[20] Z. Zha and L. Hu, Two classes of permutation polynomials over finite fields, *Finite Fields Appl.* **18** (2012), no. 4, 781-790.

[21] M. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory* **4** (2008), 851–857.

[22] M. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, *Proc. Amer. Math. Soc.* **137** (2009), no. 7, 2209-2216.

[23] M. Zieve, Classes of permutation polynomials based on cyclotomy and an additive analogue, Additive Number Theory, 355-361, Springer, New York, 2010.

School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6, CANADA
E–mail address: wang@math.carleton.ca

School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada

E-mail address: wang@math.carleton.ca